UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,485	03/09/2001	Burton S. Kaliski JR.	1048-006	5894

47654 7590 05/30/2008

BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/802,485	KALISKI, BURTON S.	
	Examiner	Art Unit	
	BEEMNET W. DADA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-20,31,38-41 and 44-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-20,31,38-41 and 44-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 14, 2008 has been entered. Claims 1, 2, 19, 38 and 47 have been amended. Claims 1, 2, 4-20, 31, 38-41and 44-51 are pending.

Response to Arguments

Applicant's arguments filed April 14, 2008 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1, 2, 4-20, 31, 38-41and 44-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Ford US 6,829,356 B1.

As per claims 1, 38 and 47, Ford teaches a method comprising:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret,

wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret [column 4, line 40-column 5, line 18 and column 9, lines 31-41];

authenticating the client by a device, the device storing an encrypted secret and configured not to provide the encrypted secret without authentication and the device being distinct from the server [column 8, lines 50-54 figure 3, step 310]; and

after authenticating, providing to the client by the device the encrypted secret, wherein the encrypted secret is capable of being decrypted using a decryption key derived from the third secret and wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret (i.e., storing encrypted user data, column 10, lines 1-15);

wherein implementing the multi-party secure computation protocol involves:

at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server [column 10, lines 29-39];

at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client [column 10, lines 39-44]; and

at the client, deriving the third secret from the intermediate data [column 10, lines 44-54].

As per claims 2 and 41, Ford further teaches the method wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function [column 10, lines 44-54].

As per claim 4, Ford further teaches the method wherein the client secret comprises at least one of a PIN, a password and biometric information [column 8, lines 54-67].

As per claims 5-7 and 44-46 Ford further teaches the method wherein the intermediate data is derived from at least the client secret and the server secret by use of a blind function evaluation protocol [column 10, lines 39-44].

As per claim 8, Ford further teaches the method wherein authenticating comprises authenticating the client based on a time-dependent code [column 8, lines 50-54].

As per claim 9, Ford further teaches the method wherein authenticating comprises authenticating the client based on at least one of a PIN, a password and biometric information [column 8, lines 50-54].

As per claim 10, Ford further teaches the method wherein authenticating comprises authenticating the client based on a secret other that the client secret [column 8, lines 50-54].

As per claim 11, Ford further teaches the method wherein authenticating comprises using an authenticating secret derived from the third secret [column 8, lines 50-54].

As per claims 12 and 13, Ford further teaches the method wherein the device comprise at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card and a desktop computer [figures 1-3].

As per claims 14-16, Ford further teaches the method wherein the encrypted secret comprises an encrypted private key of a public/private key pair used for asymmetric cryptography [column 10, lines 1-15].

As per claim 17, Ford further teaches the method wherein the encrypted secret comprises an encrypted secret key used for symmetric cryptography [column 10, lines 1-15].

As per claim 18, Ford further teaches the method wherein the encrypted secret comprises at least one unit of encrypted digital currency [column 10, lines 1-15].

As per claims 19 and 20, Ford further teaches the method further comprising verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data [column 10, lines 39-44].

As per claim 31, Ford further teaches the method further comprising deriving the decryption key from a third secret, and decrypting the encrypted secret using the decryption key [column 10, lines 39-54].

As per claim 39, Ford further teaches the method further comprising transmitting to the first server by the network server verification that the user has authenticated successfully [column 8, lines 50-54 and figure 3, step 310].

As per claim 40, Ford further teaches the method wherein the network server is a web server [figures 1-3].

As per claim 48, Ford further teaches the method wherein the password is derived from the third secret and a server identifier [column 10, lines 39-54].

As per claims 49-51, Ford further teaches the method wherein the multi-party secure computation protocol comprises the client and the server providing their respective secrets as input into to respective protocol operations that jointly calculate the third secret as a function of the client and server secrets [figures 3 and 4].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/

May 20, 2008
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135